



ACOS Venafi Integration Guide

February, 2024

© 2024 A10 Networks, Inc All rights reserved.

Information in this document is subject to change without notice.

PATENT PROTECTION

A10 Networks, Inc products are protected by patents in the U.S. and elsewhere. The following website is provided to satisfy the virtual patent marking provisions of various jurisdictions including the virtual patent marking provisions of the America Invents Act. A10 Networks, Inc products, including all Thunder Series products, are protected by one or more of U.S. patents and patents pending listed at:

[a10-virtual-patent-marking](#).

TRADEMARKS

A10 Networks, Inc trademarks are listed at: [a10-trademarks](#)

DISCLAIMER

This document does not create any express or implied warranty about A10 Networks, Inc or about its products or services, including but not limited to fitness for a particular use and non-infringement. A10 Networks, Inc has made reasonable efforts to verify that the information contained herein is accurate, but A10 Networks, Inc assumes no responsibility for its use. All information is provided "as-is." The product specifications and features described in this publication are based on the latest information available; however, specifications are subject to change without notice, and certain features may not be available upon initial product release. Contact A10 Networks, Inc for current information regarding its products or services. A10 Networks, Inc products and services are subject to A10 Networks, Inc standard terms and conditions.

ENVIRONMENTAL CONSIDERATIONS

Some electronic components may possibly contain dangerous substances. For information on specific component types, please contact the manufacturer of that component. Always consult local authorities for regulations regarding proper disposal of electronic components in your area.

FURTHER INFORMATION

For additional information about A10 products, terms and conditions of delivery, and pricing, contact your nearest A10 Networks, Inc location, which can be found by visiting www.a10networks.com.

Table of Contents

- Overview 4
- Integration with Venafi 5
 - Prerequisites 5
 - PowerShell Script Installation 6
 - Onboard Discovery of Applications and Certificates 8
 - Prerequisites 8
 - Creating an Onboard Discovery Job11
 - Executing the Onboard Discovery Job15
 - Certificate Renewal17
 - Prerequisites17
 - Renewing Discovered Certificates18
- Support 20

Overview

The creation or renewal of digital certificates involves several steps, multiple teams, and offers less visibility into expiring or noncompliant certificates.

Venafi demonstrates proven interoperability with A10 Thunder ADC to provide the customers with a consolidated and simplified method to manage critical security information, such as certificate locations, key sizes, ciphers used, and validity dates. This solution provides a complete view of an organization's digital certificates and makes it easy to fully automate the use of keys and certificates as the business grows.

The purpose of this document is to provide the steps to integrate A10 devices with Venafi Trust Protection Platform and automate certificate renewal. The overall process is described as follows:

1. Download and install the PowerShell script from the Venafi marketplace. See [PowerShell Script Installation](#).
2. Create a Credential Object to authenticate the connection to the A10 device. See [Prerequisites](#).
3. Create a Device object to reference the A10 device and validate its certificates and private keys. See [Prerequisites](#).
4. Create and execute an Onboard Discovery job to discover and import the applications and certificates into the Venafi platform. See [Creating an Onboard Discovery Job](#).
5. Automate the renewal of expired certificates. The renewed certificates are downloaded and installed on the A10 device automatically. See [Certificate Renewal](#).

Integration with Venafi

The following topics are covered in this section:

Prerequisites	5
PowerShell Script Installation	6
Onboard Discovery of Applications and Certificates	8
Certificate Renewal	17

Prerequisites

Before performing the integration steps, ensure the following:

- Venafi Trust Protection Platform is installed and configured.

This platform rapidly develops an accurate certificate inventory and identifies security and operational risks.

- Connectivity between the Trust Protection Platform and Thunder device.
- A10 policy folder is created in the Venafi Trust Protection Platform.

It's a separate logical container for the A10 devices and policies inside the platform. To create the policy folder, see [Venafi documentation](#).

- ACOS Thunder device is set up with a basic configuration.

In this document, it is assumed that the device is configured with a virtual server, having a virtual port with the Template Client SSL certificate associated with it.

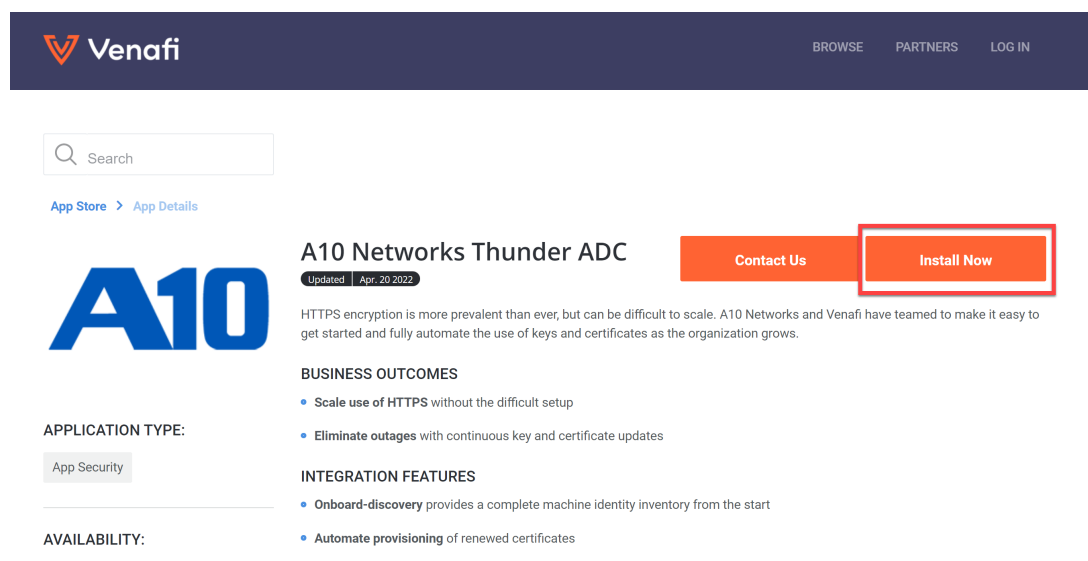
PowerShell Script Installation

You need to download and install the PowerShell script from the Venafi marketplace. This script provides routines that are invoked to conduct programmed operations in response to the Trust Protection Platform events at various phases of the certificate lifecycle.

To install the PowerShell script:

1. Go to the Venafi [marketplace](#) website.
2. Click **Install Now** (as shown in [Figure 1](#)).

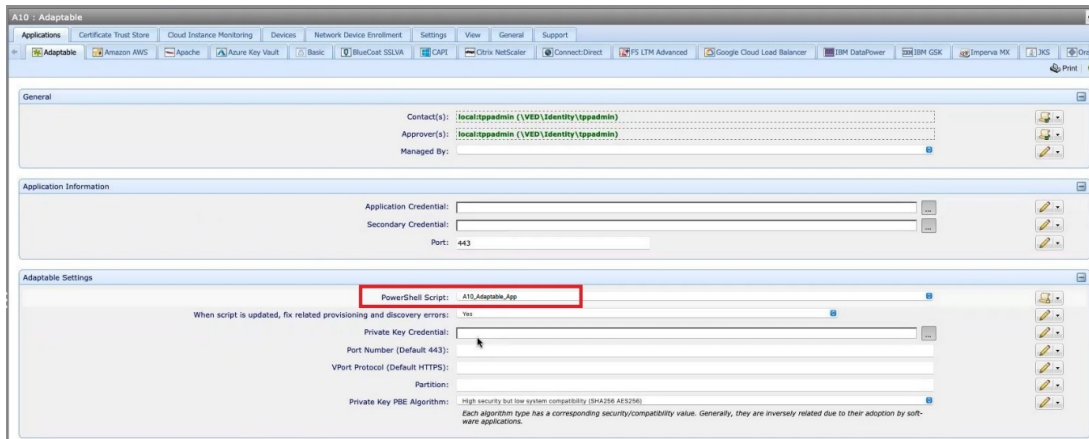
Figure 1 : Venafi marketplace



3. Unzip the downloaded file.
4. Place the script (A10_Adaptable_App.ps1) in the **Program Files\Venafi\Scripts\AdaptableApp** folder of your Venafi windows server instance.
5. Access Venafi Trust Protection Platform through the web browser.
6. From the menu bar, click **Policy Tree** and open the **A10** policy folder.
7. Navigate to **Applications > Adaptable > Adaptable Settings > PowerShell Script**.

8. Select **A10_Adaptable_App** script from the combo-box.

The A10 policy folder uses this script for all purposes.



The screenshot shows the 'A10 - Adaptable' configuration window. The 'Adaptable Settings' tab is active. The 'PowerShell Script' dropdown menu is highlighted with a red box, showing 'A10_Adaptable_App' selected. Other fields include 'Contact(s)', 'Approver(s)', 'Managed By', 'Application Credential', 'Secondary Credential', 'Port' (443), 'Private Key Credential', 'Port Number (Default 443)', 'VPort Protocol (Default HTTPS)', 'Partition', and 'Private Key PBE Algorithm'.

Onboard Discovery of Applications and Certificates

The Onboard Discovery feature automates the process of importing certificates from the A10 devices into the Trust Protection Platform so you can monitor, validate, and provision them.

This section describes the steps to create and execute an Onboard Discovery job.

The following topics are covered:

Prerequisites	8
Creating an Onboard Discovery Job	11
Executing the Onboard Discovery Job	15

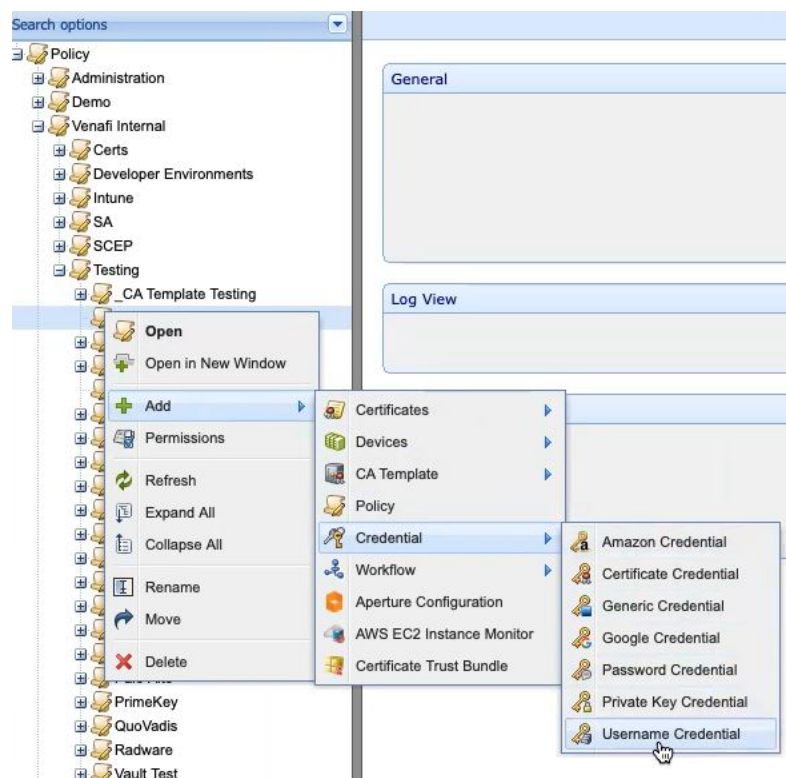
Prerequisites

Before running the onboard discovery job, ensure the following tasks are performed:

1. Create a credential object on the Trust Protection Platform to authenticate the A10 device.

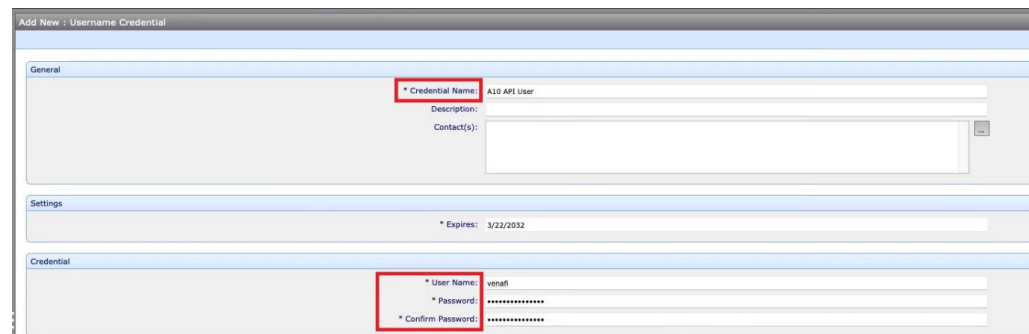
To create a credential object:

- a. Open the **Policy Tree** view.
- b. Click **A10** policy and right click to select **Add > Credential > Username Credential**.



The **Username Credential** page is displayed ([Figure 2](#)).

Figure 2 : Username Credential page


 A screenshot of the 'Add New : Username Credential' page in the Venafi console. The page has three main sections: 'General', 'Settings', and 'Credential'. In the 'General' section, the '* Credential Name:' field is highlighted with a red box and contains the text 'A10 API User'. In the 'Credential' section, the '* User Name:' field (containing 'venafi') and the '* Password:' field (containing masked characters) are both highlighted with red boxes. The '* Confirm Password:' field is also visible below the password field.

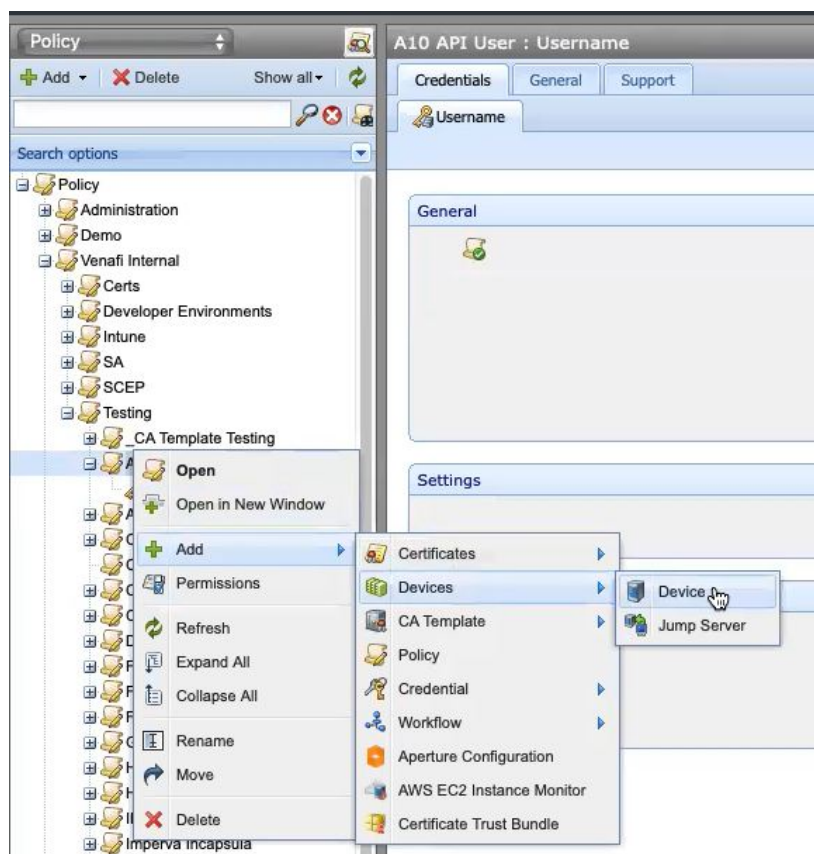
- c. In the **General** section, enter a credential object name in the **Credential Name** field.
- d. In the **Credential** section, enter a username and password in the respective fields.

NOTE: Enter the same credentials that are used to login to the A10 Thunder device.

- e. Click **Save**.
2. Create a device object on the Trust Protection Platform to reference the A10 device and validate its certificates and private keys.

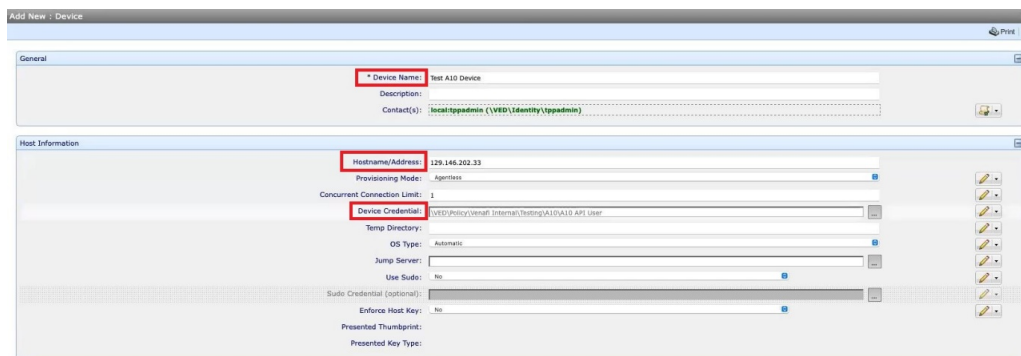
To create a device object:

- a. Open the **Policy Tree** view.
- b. Click **A10** policy and right click to select **Add > Devices > Device**.



The **Device** page is displayed ([Figure 3](#)).

Figure 3 : Device page



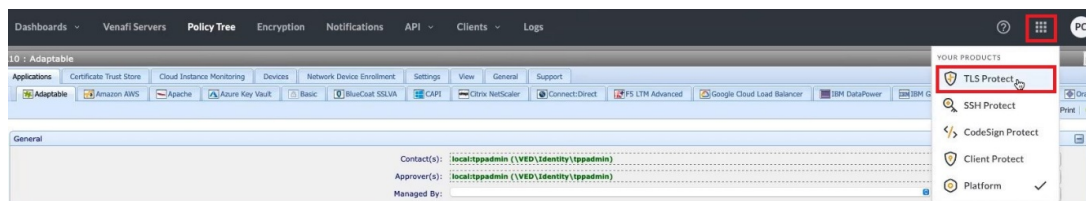
- c. In the **General** section, enter a name in the **Device Name** field.
- d. In the **Host Information** section, enter the IP address of the A10 device.
- e. In the **Device Credential** field, specify the credential object (created in [Step 1](#)). This object is used to authenticate the connection with the A10 device.
- f. Click **Save**.

For more information, see [Device Object Setting](#).

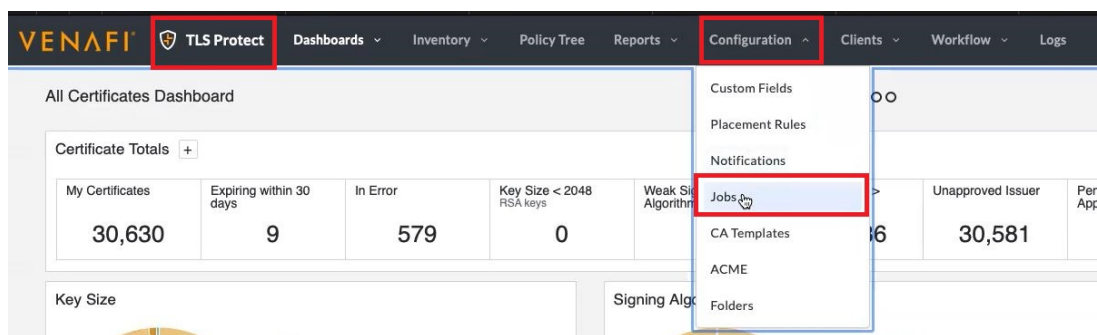
Creating an Onboard Discovery Job

To create an Onboard Discovery job:

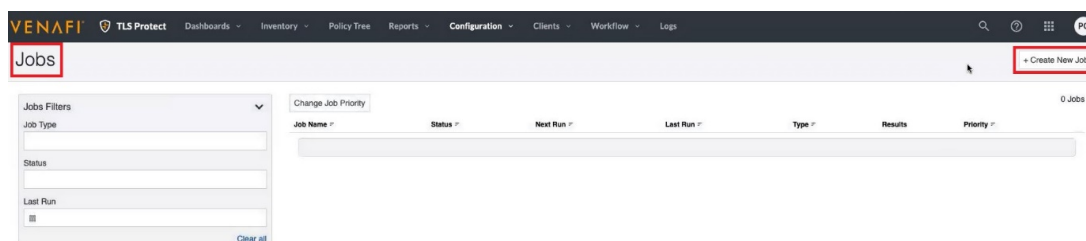
1. Open the **TLS Protect** management interface on the Trust Protection Platform.



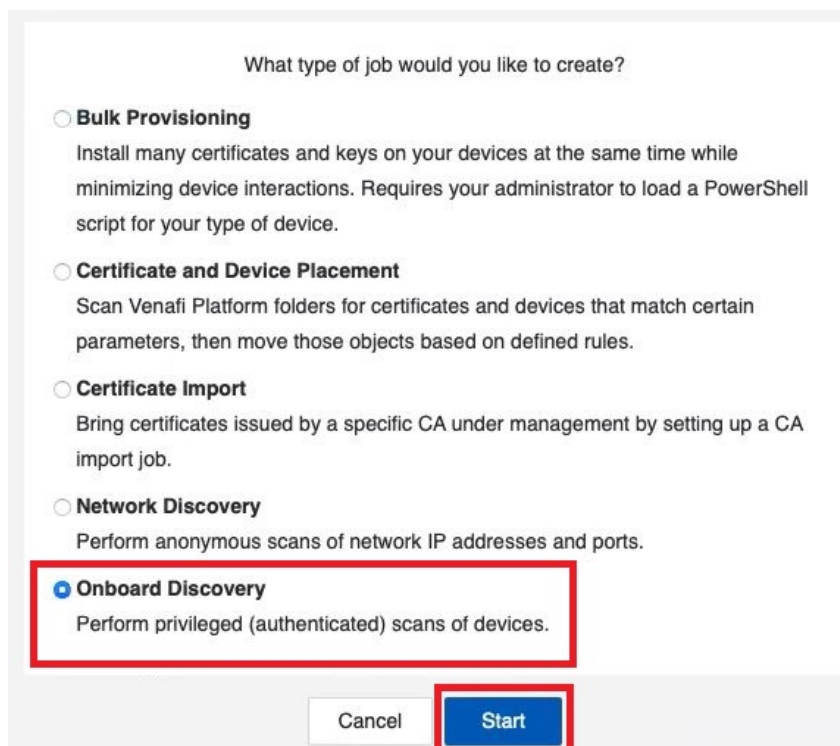
2. Navigate to **Configuration > Jobs**.



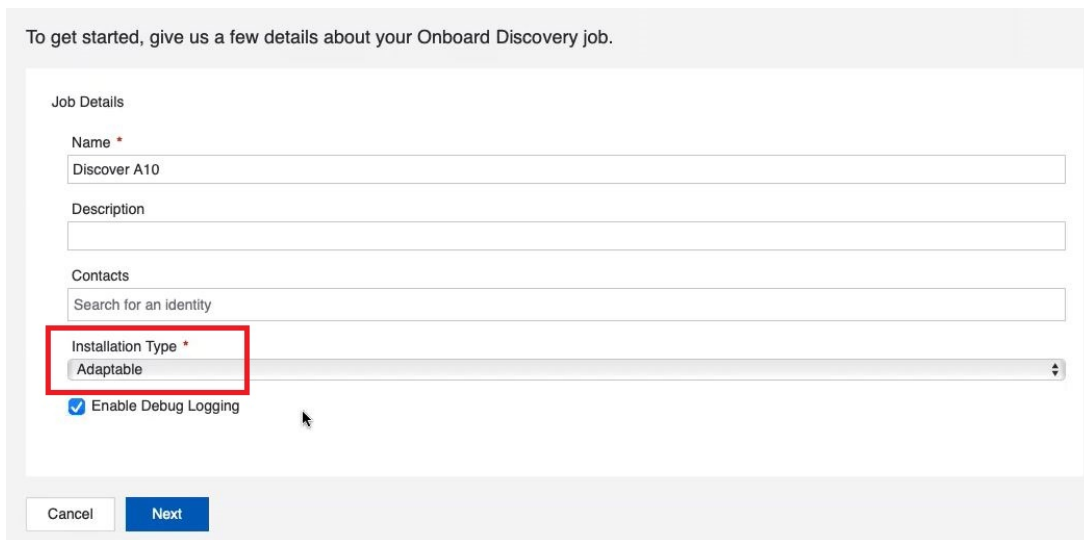
3. Click **+ Create New Job** to start the **Create New Job** wizard.



4. On the **Create New Job** page, select **Onboard Discovery**, and then click **Start**.



The **Job Details** page is displayed.



To get started, give us a few details about your Onboard Discovery job.

Job Details

Name *
Discover A10

Description

Contacts
Search for an identity

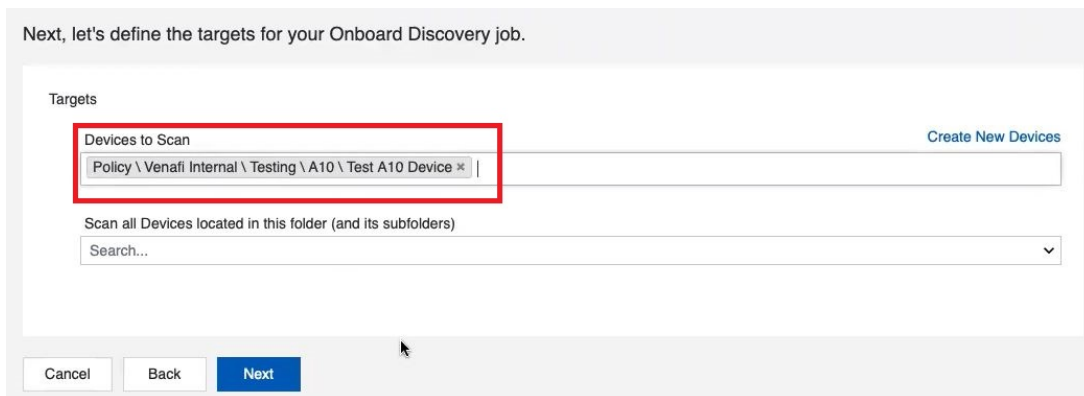
Installation Type *
Adaptable

☒ Enable Debug Logging

Cancel Next

5. In the **Name** field, enter a name for your new onboard discovery job.
6. In the **Description** field, enter a description that describes the purpose for this new job (this is optional).
7. In the **Contacts** field, enter the contact names for your new job (this is optional).
8. In the **Installation Type** list field, select the installation type as **Adaptable** and click **Next**.

The **Targets** page is displayed.



Next, let's define the targets for your Onboard Discovery job.

Targets

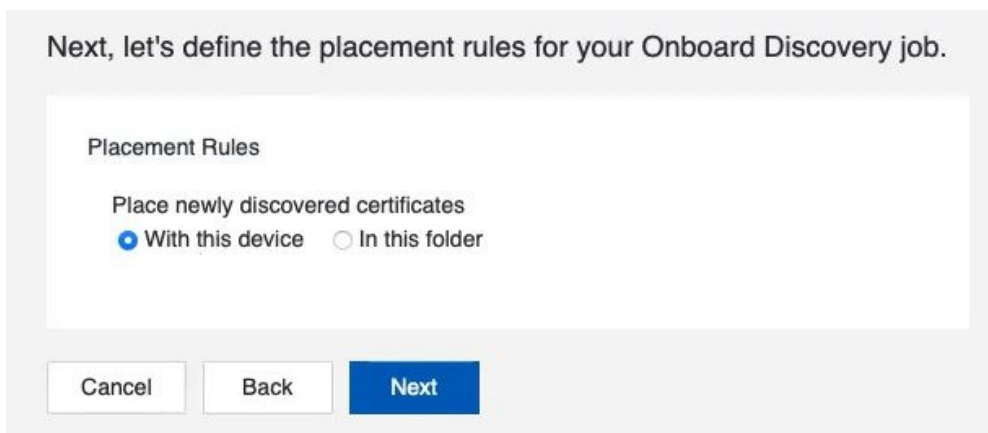
Devices to Scan Create New Devices
Policy \ Venafi Internal \ Testing \ A10 \ Test A10 Device

Scan all Devices located in this folder (and its subfolders)
Search...

Cancel Back Next

9. In the **Devices to Scan** field, select the device object created [previously](#) and click **Next**.

The **Placement Rules** page is displayed.



Next, let's define the placement rules for your Onboard Discovery job.

Placement Rules

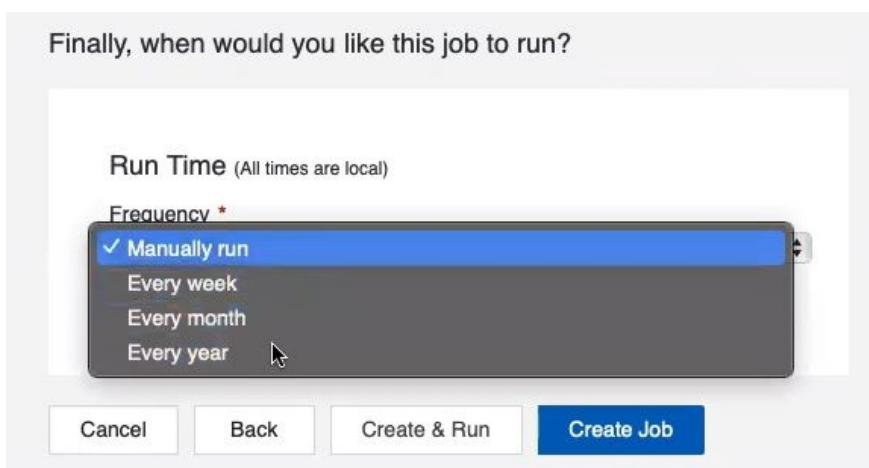
Place newly discovered certificates

☒ With this device ☐ In this folder

Cancel Back Next

10. On the **Placement Rules** page, select one of the following,
 - **With this device** – Stores all the newly discovered certificates in the same folder where the device is located.
 - **In this folder** – Stores all the newly discovered certificates in the folder you specify (in the field below).
11. Click **Next**.

The **Run Time** page is displayed.



Finally, when would you like this job to run?

Run Time (All times are local)

Frequency *

✓ Manually run
Every week
Every month
Every year

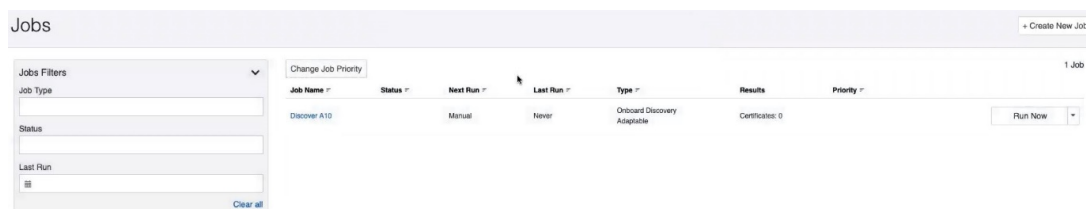
Cancel Back Create & Run Create Job

12. On the **Run Time** page, set the **Frequency** for running the job by selecting one of the following,

- **Every week / Every month / Every year** – Sets a recurring time for the job to regularly synchronize the inventories by discovering newly added certificates.
- **Manually run** – Executes the job manually whenever required.

13. Click **Create Job**.

The job is created and displayed under the jobs list on the **Jobs** page.



The screenshot shows the 'Jobs' page interface. On the left, there is a 'Jobs Filters' sidebar with fields for 'Job Type', 'Status', and 'Last Run', along with a 'Clear all' button. The main area features a 'Change Job Priority' button and a table with columns: 'Job Name', 'Status', 'Next Run', 'Last Run', 'Type', 'Results', and 'Priority'. A single job is listed: 'Discover A10' with status 'Manual', next run 'Never', type 'Onboard Discovery Adaptable', and results 'Certificates: 0'. A 'Run Now' button is visible at the end of the row.

Executing the Onboard Discovery Job

To execute the discovery job:

1. After the job is created and displayed on the Jobs page, click Run Now.



This screenshot is identical to the previous one, but the 'Run Now' button at the end of the 'Discover A10' job row is highlighted with a red rectangular box.

When the execution is complete, the Discovery page displays the Status as Complete. Additionally, the New Applications and New Certificates fields display the number of applications and certificates discovered on the device.

Discover A10

Discovery\

Results

Details and Targets

Schedule

Permissions


Results

Status	Complete
Last Run	3/22/2022 8:46 AM (-07:00 UTC)
New Applications	1
New Certificates	1
New Keys	0

Devices

Pending	0
In Progress	0
Failed	0
Completed	1
Aborted	0

2. To view the newly discovered applications and associated certificates, switch to the Policy Tree view and refresh it.



The Policy Tree view shows a hierarchy of folders. Under 'A10', there are two items highlighted with red boxes: 'vs-1' (a certificate) and 'Test A10 Device' (an application). Red arrows point from these items to labels on the right: 'Discovered Certificate' for 'vs-1' and 'Discovered Application' for 'Test A10 Device'.

Discovered Certificate

Discovered Application

NOTE: During onboard discovery, only the public section of the certificates and the metadata required for provisioning the certificates are imported. The Venafi Trust Protection Platform does not import or store the private key.

Certificate Renewal

Certificate renewal is the process of purchasing a new certificate for the same public key that was used in the expired certificate. After renewal, the new certificate is automatically downloaded and installed on the device.

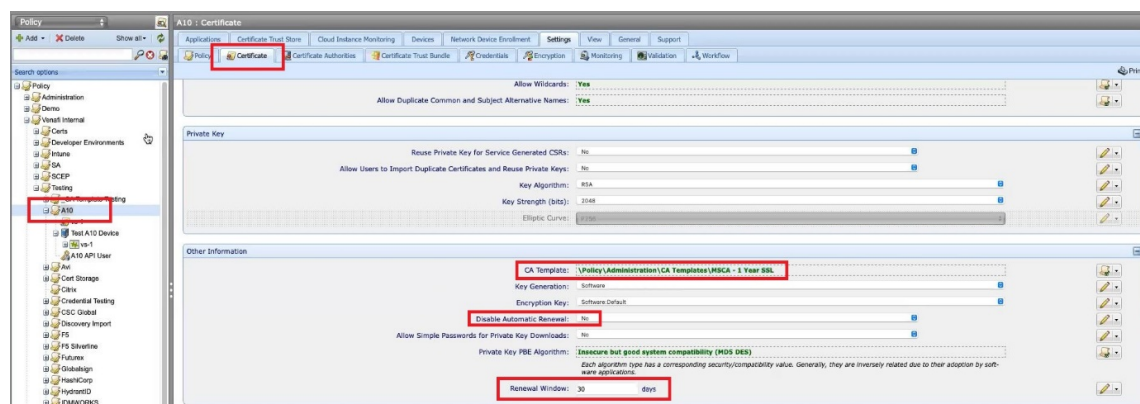
This section describes the steps to renew the expired certificates.

The following topics are covered:

Prerequisites	17
Renewing Discovered Certificates	18

Prerequisites

Before renewing the certificates, ensure that the **Certificate Authority (CA) template** is configured under the A10 certificate policy (as shown in the figure below). For steps to create and configure the Certification Authority (CA) template, see [Configuring Certificate Authority](#).



The CA template object contains information required for the Trust Protection Platform to connect to the CA for certificate management.

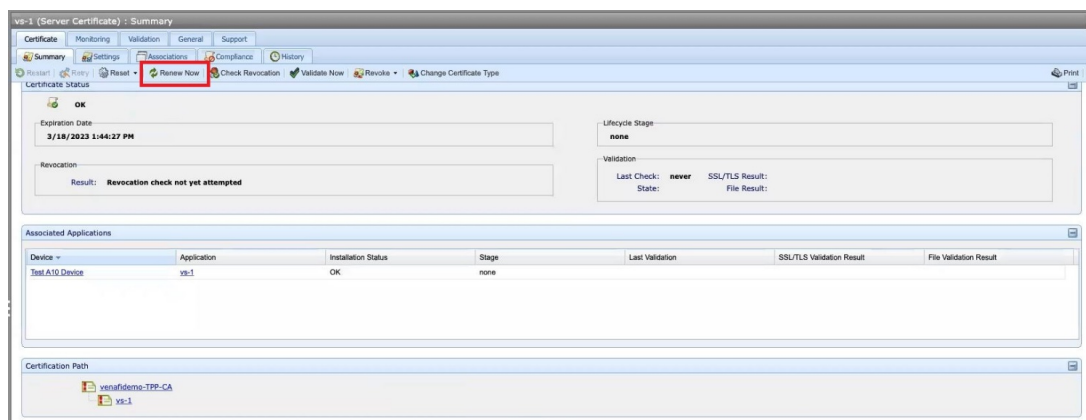
Additionally, the certificate renewal behavior is affected by certain options configured under the A10 Certificate policy. Hence, ensure that the following options are configured correctly,

- **Disable automatic renewal:** By default, automatic renewal is enabled for certificates in the Trust Protection Platform. To disable automatic renewal, set this value to **Yes**.
- **Renewal window:** This parameter indicates the number of days before expiration, to renew the certificates. It is recommended to set this value between 30 to 90 days to ensure that there is enough time to complete the processes and necessary approvals for renewing the certificate before the old certificate expires.

Renewing Discovered Certificates

To renew the discovered certificate:

1. Open the certificate in the **Policy Tree** view and click **Renew Now**.



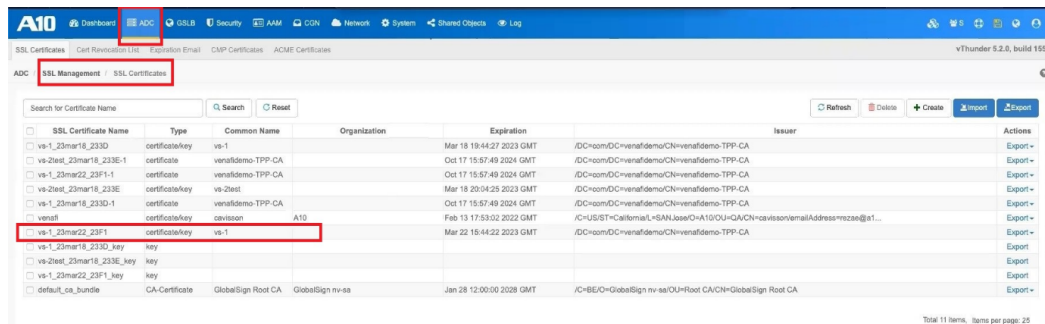
2. On the confirmation pop-up, click **Yes** to commence the certificate renewal process.



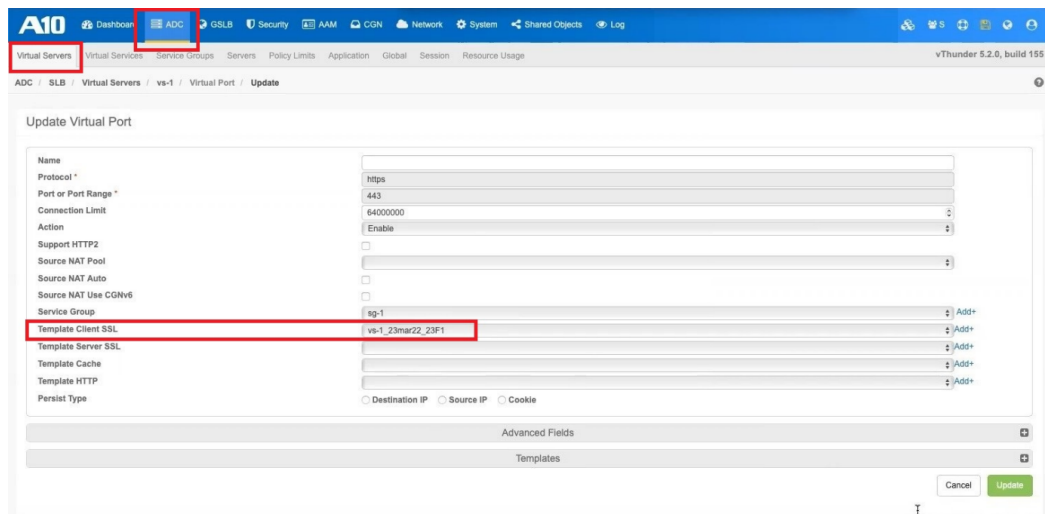
The following processes take place in the background:

- a. The Trust Protection Platform creates a private key and generates the certificate signing request (CSR).
- b. The CSR is forwarded to the configured Certificate Authority (CA).

- c. The Trust Protection Platform retrieves the new signed certificate and key from the CA.
 - d. The new signed certificate and private key is sent to the A10 device and installed automatically.
3. Verify new certificate installation by checking the certificate information in the A10 interface.
 - A. To check the renewed certificate information, navigate to **ADC > SSL Management > SSL Certificates**.



- B. The renewed certificate is also associated with the virtual port configuration replacing the old certificate. To check this config, navigate to **ADC > SLB > Virtual Server > Virtual Port > Edit > Template Client SSL**.



For more information, see [Certificate Renewal](#).

Support

For more information about A10 Thunder products, contact A10 Networks at:
<https://www.a10networks.com/contact-us/>.

For technical assistance, contact A10 Networks Technical Support by following the instructions at: <https://support.a10networks.com/>.



©2024 A10 Networks, Inc All rights reserved. A10 Networks, the A10 Networks logo, ACOS, A10 Thunder, Thunder TPS, A10 Harmony, SSLi and SSL Insight are trademarks or registered trademarks of A10 Networks, Inc. in the United States and other countries. All other trademarks are property of their respective owners. A10 Networks assumes no responsibility for any inaccuracies in this document. A10 Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice. For the full list of trademarks, visit: www.a10networks.com/company/legal/trademarks/.